

EXHIBIT B

U.S. Patent No. 7,844,718 V. Microsoft Corporation

1. Claim Chart

Claim	Analysis
<p>[1.P] A method of configuring a remote computer to access a network of computers, comprising:</p>	<p>Microsoft Corporation (“Defendant”) performs and/or induces others to perform a method configuring a remote computer to access a network of computers.</p> <p>This element is infringed literally, or in the alternative, under the doctrine of equivalents.</p> <p>For example, Defendant provides Intune which has the capability to remotely configure multiple devices such as computers, laptops, and/or notebooks (running on Windows 10 and 11 only). Further, Intune allows an admin to configure a remote computer for a Virtual Private Network (VPN) (“network of computers”) by deploying VPN profiles.</p> <p>Microsoft Intune is a cloud-based endpoint management solution. It manages user access and simplifies app and device management across your many devices, including mobile devices, desktop computers, and virtual endpoints.</p> <p>Source: https://learn.microsoft.com/en-us/mem/intune/fundamentals/what-is-intune</p> <p>These products and services offer a cloud-based unified endpoint management solution. It simplifies management across multiple operating systems, cloud, on-premises, mobile, desktop, and virtualized endpoints. It also:</p> <p>Source: https://learn.microsoft.com/en-us/mem/endpoint-manager-overview</p> <p>Virtual private networks (VPNs) give users secure remote access to your organization network. Devices use a VPN connection profile to start a connection with the VPN server. VPN profiles in Microsoft Intune assign VPN settings to users and devices in your organization. Use these settings so users can easily and securely connect to your organizational network.</p> <p>Source: https://learn.microsoft.com/en-us/mem/intune/configuration/vpn-settings-configure</p>

Windows 10/11 and Windows Holographic device settings to add VPN connections using Intune

Source: <https://learn.microsoft.com/en-us/mem/intune/configuration/vpn-settings-windows-10>

Further, to the extent this element is performed at least in part by Defendant's software source code, Plaintiff shall supplement these contentions pursuant to production of such source code by the Defendant.

[1.1] initiating, at a network administrator computer of the network of computers, an installer program having an empty binary file, the installer program being configured to generate an executable file using the binary file when the empty binary file is populated;

Defendant performs and/or induces others to perform the step of initiating, at a network administrator computer of the network of computers, an installer program having an empty binary file, the installer program being configured to generate an executable file using the binary file when the empty binary file is populated.

This element is infringed literally, or in the alternative, under the doctrine of equivalents.

For example, Intune comprises an admin center accessible on the admin's device. Through the admin center, Intune allows an admin to configure a remote computer with VPN ("network of computers") by creating and deploying VPN Profiles. A VPN profile can be created by adding the information from a ProfileXML file in the Base VPN section, where the ProfileXL file contains multiple data fields (such as Platform, Profile, and Configuration settings).

Upon information and belief, the admin center includes an empty binary file which is populated when the information from the ProfileXML file is added, and an executable file is generated to be executed at the remote computer, by an installer program in the admin center.

Apply ProfileXML using Intune

After you configure the settings that you want using ProfileXML, you can create a custom profile in the [Microsoft Intune admin center](#). After it's created, you deploy this profile to your devices.

1. Sign in to the [Microsoft Intune admin center](#).

2. Select **Devices > Configuration profiles > Create profile**.

3. Enter the following properties:

- **Platform:** Select **Windows 10 and later**
- **Profile:** Select **Templates > Custom**.

4. Select **Create**.

5. In **Basics**, enter the following properties:

- **Name:** Enter a descriptive name for the profile. Name your profiles so you can easily identify them later.
- **Description:** Enter a description for the profile. This setting is optional, but recommended.

6. Select **Next**.

7. In **Configuration settings**, enter the following properties:

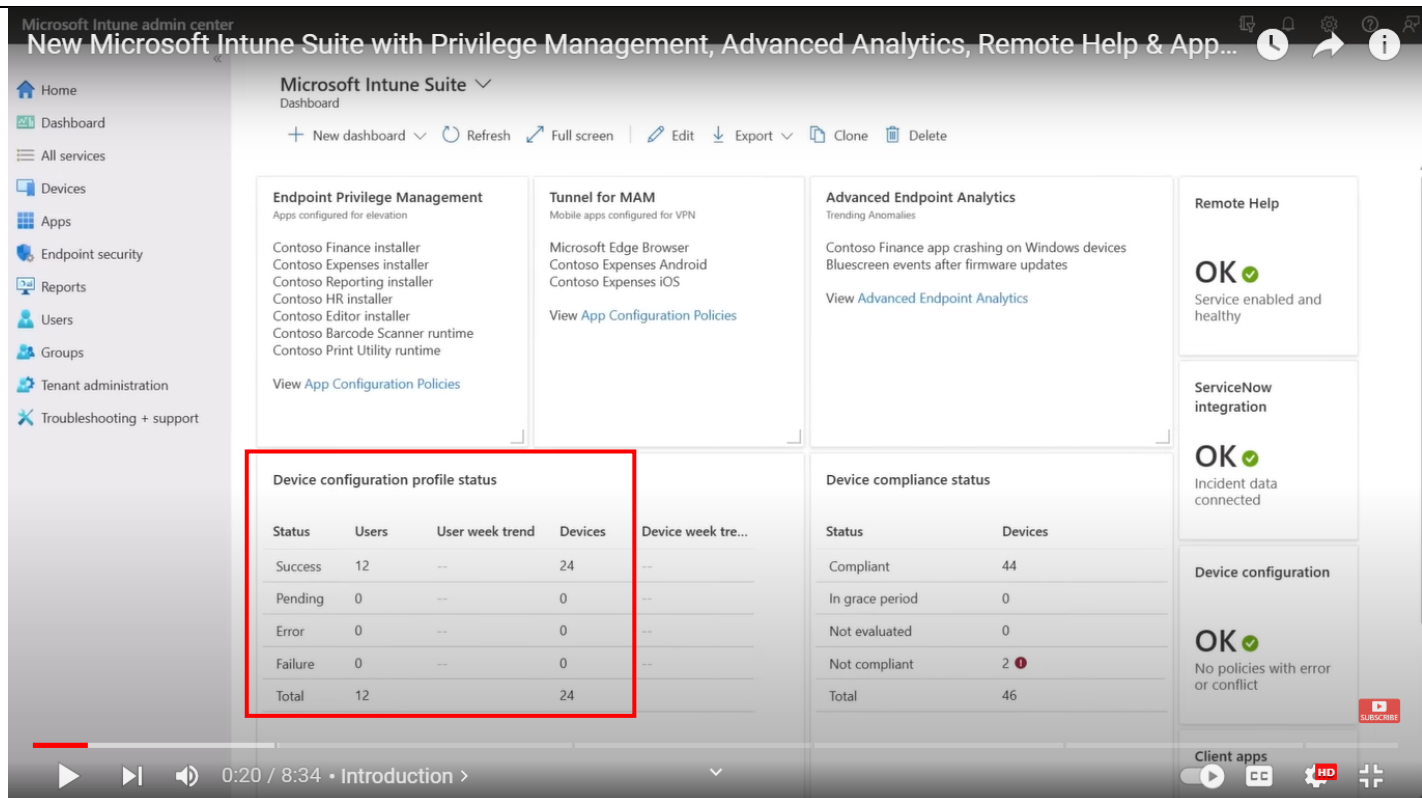
- **OMA-URI:** Enter `./user/vendor/MSFT/VPNv2/Your_VPN_profile_name_/ProfileXML`.
- **Data type:** Select `String (XML file)`.
- **Value:** Browse to, and select your XML file.

Source: <https://learn.microsoft.com/en-us/windows/security/operating-system-security/network-security/vpn/vpn-profile-options#apply-profilexml-using-intune>

Your administrative account will need specific permissions in order to access the Microsoft Managed Desktop administrative features in the Microsoft Intune admin center².

You can manage admin access to these features within your organization by using role-based access control. Several Azure Active Directory (Azure AD) administrator roles, and built-in Microsoft Managed Desktop roles are available to provide more granular control to different features within the Microsoft Intune admin center². For more information about Azure Active Directory roles, see [Azure AD built-in roles](#).

Source: <https://learn.microsoft.com/en-us/managed-desktop/prepare/access-admin-center>



Source: <https://www.youtube.com/watch?v=nEa5AFBCRbI> at 0:20.

Further, to the extent this element is performed at least in part by Defendant's software source code, Plaintiff shall supplement these contentions pursuant to production of such source code by the Defendant.

[1.2] accessing, at the network administrator computer, a network database using a user data application to extract configuration data that represents binary settings

Defendant performs and/or induces others to perform the step of accessing, at the network administrator computer, a network database using a user data application to extract configuration data that represents binary settings of a network topology and binary settings of the remote computer.

This element is infringed literally, or in the alternative, under the doctrine of equivalents.

of a network topology and binary settings of the remote computer;

For example, Intune admin center allows the admin to import configuration data in the form of ProfileXML file (“network database”). Upon information and belief, the contents of such ProfileXML file comprise configuration data including binary settings of the network topology such as IP Address, DNS Tunneling, Proxy, and binary settings of the remote computer such as Platform or operating system of the remote computer.

You can add and configure VPN connections for devices using Microsoft Intune. This article describes some of the settings and features you can configure when creating virtual private networks (VPNs). These VPN settings are used in device configuration profiles, and then pushed or deployed to devices.

Source: <https://learn.microsoft.com/en-us/mem/intune/configuration/vpn-settings-windows-10>

```
PowerShell Copy

# Define key VPN profile parameters
# Replace with your own values

$Domain = 'corp' # Name of the domain.

$TemplateName = 'Contoso VPN' # Name of the test VPN connection you created in the tutorial.

$ProfileName = 'Contoso AlwaysOn VPN' # Name of the profile we are going to create.

$Servers = 'aov-vpn.contoso.com' #Public or routable IP address or DNS name for the VPN gateway.

$DnsSuffix = 'corp.contoso.com' # Specifies one or more commas separated DNS suffixes.

$DomainName = '.corp.contoso.com' #Used to indicate the namespace to which the policy applies. Contains

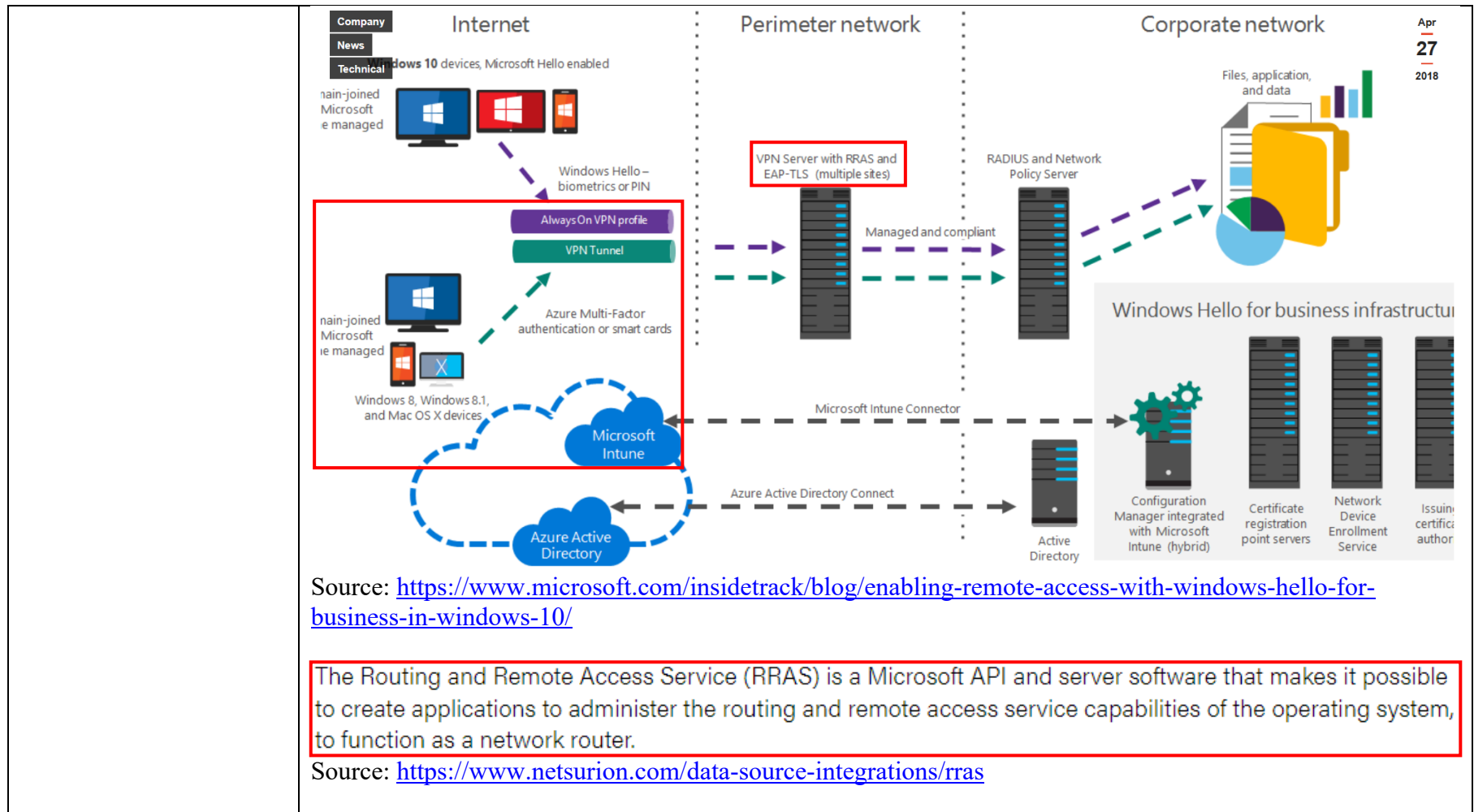
$DNSServers = '10.10.0.6' #List of comma-separated DNS Server IP addresses to use for the namespace.

$TrustedNetwork = 'corp.contoso.com' #Comma-separated string to identify the trusted network.
```

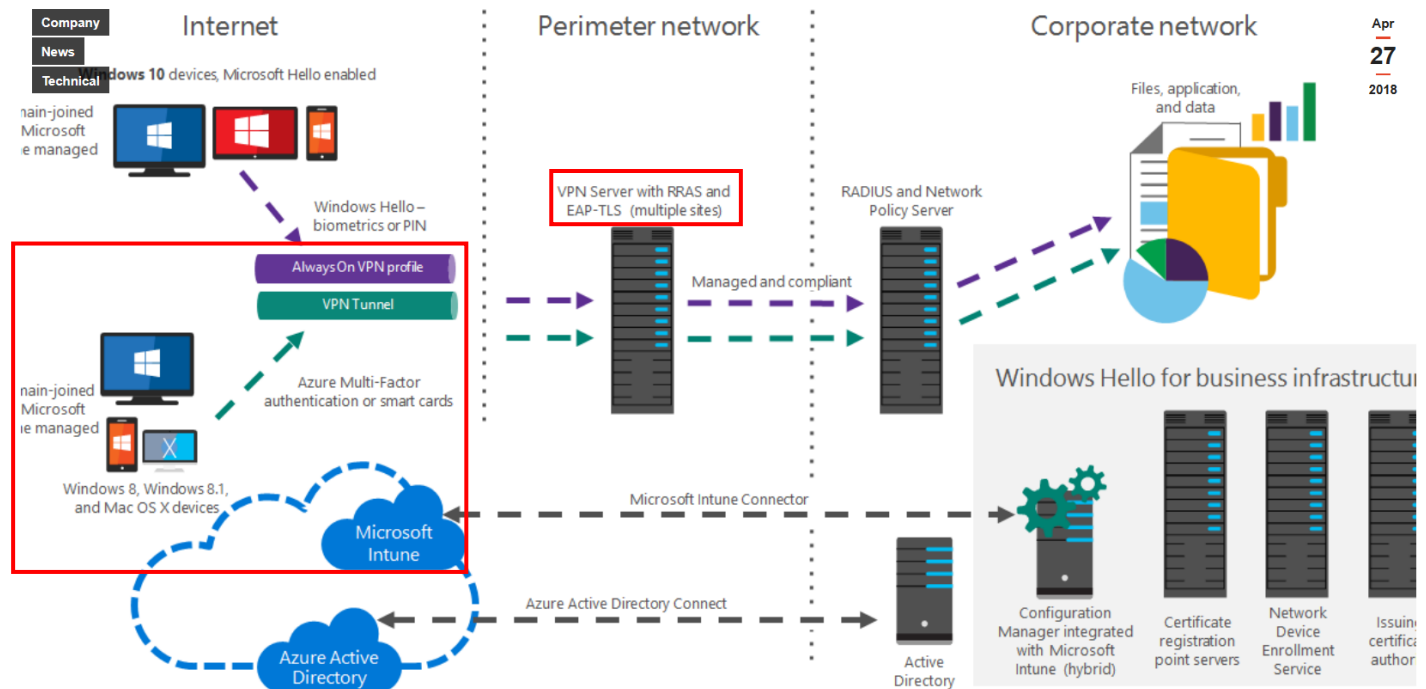
Source: <https://learn.microsoft.com/en-us/windows-server/remote/remote-access/tutorial-aovpn-deploy-configure-client>

	<p>3. Enter the following properties:</p> <ul style="list-style-type: none"> • Platform: Choose the platform of your devices. Your options: <ul style="list-style-type: none"> ◦ Android device administrator ◦ Android Enterprise > Fully Managed, Dedicated, and Corporate-Owned Work Profile ◦ Android Enterprise > Personally-owned work profile ◦ iOS/iPadOS ◦ macOS ◦ Windows 10 and later ◦ Windows 8.1 and later • Profile: Select VPN. Or, select Templates > VPN. <p>Source: https://learn.microsoft.com/en-us/mem/intune/configuration/vpn-settings-configure</p> <ul style="list-style-type: none"> • Register IP addresses with internal DNS: Select Enable to configure the VPN profile to dynamically register the IP addresses assigned to the VPN interface with the internal DNS. Select Disable to not dynamically register the IP addresses. <p>Source: https://learn.microsoft.com/en-us/mem/intune/configuration/vpn-settings-windows-10</p> <p>Further, to the extent this element is performed at least in part by Defendant's software source code, Plaintiff shall supplement these contentions pursuant to production of such source code by the Defendant.</p>
<p>[1.3] applying, at the network administrator computer, the binary settings of the network topology and the binary setting of the remote computer to code a</p>	<p>Defendant performs and/or induces others to perform the step of applying, at the network administrator computer, the binary settings of the network topology and the binary setting of the remote computer to code a Remote Access Service (RAS) Application Programming Interface (API) to generate a configuration data binary file and prescribed RAS settings.</p> <p>This element is infringed literally, or in the alternative, under the doctrine of equivalents.</p>

<p>Remote Access Service (RAS) Application Programming Interface (API) to generate a configuration data binary file and prescribed RAS settings;</p>	<p>For example, when the admin clicks on “Create” while making the VPN profile, upon information and belief, Intune uses the configuration data such as DNS server address, Domain data (“binary settings of a network topology”), and Platform (“binary settings of the remote computer”) to generate a configuration data binary file by coding Remote Access Service (“RAS”) Application Program Interface (“API”). The RAS API is coded to generate connection application for the remote computer such that the remote computer accesses the Remote Service through VPN.</p> <h2 data-bbox="546 487 798 568">Purpose</h2> <div data-bbox="546 584 1827 828"><p>Use Remote Access Service (RAS) to create client applications. These applications display RAS common dialog boxes, manage remote access connections and devices, and manipulate phone-book entries. RAS also provides the next generation of server functionality for the Remote Access Service (RAS) for Windows. The RRAS server functionality follows and builds upon the Remote Access Service (RAS).</p></div> <h2 data-bbox="546 876 1029 958">Where applicable</h2> <div data-bbox="546 974 1827 1201"><p>The Remote Access Service is applicable in any computing environment that uses a Wide Area Network (WAN) link or a Virtual Private Network (VPN). RAS makes it possible to connect a remote client computer to a network server over a WAN link or a VPN. The remote computer then functions on the server's LAN as though the remote computer was connected to the LAN directly. The RAS API enables programmers to access the features of RAS programmatically.</p></div> <p data-bbox="546 1218 1680 1266">Source: https://learn.microsoft.com/en-us/windows/win32/rras/remote-access-start-page</p>
--	--



	<h2>Routing and Remote Access Service (RRAS)</h2> <p>Article • 08/31/2016</p> <p>The Routing and Remote Access service (RRAS) supports remote user or site-to-site connectivity by using virtual private network (VPN) or dial-up connections.</p> <p>Source: https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn614140(v=ws.11)</p> <ul style="list-style-type: none">• Register IP addresses with internal DNS: Select Enable to configure the VPN profile to dynamically register the IP addresses assigned to the VPN interface with the internal DNS. Select Disable to not dynamically register the IP addresses. <p>Source: https://learn.microsoft.com/en-us/mem/intune/configuration/vpn-settings-windows-10</p> <p>Further, to the extent this element is performed at least in part by Defendant's software source code, Plaintiff shall supplement these contentions pursuant to production of such source code by the Defendant.</p>
<p>[1.4] embedding, at the network administrator computer, the configuration data binary file as instructions in the RAS API;</p>	<p>Defendant performs and/or induces others to perform the step of embedding, at the network administrator computer, the configuration data binary file as instructions in the RAS API.</p> <p>This element is infringed literally, or in the alternative, under the doctrine of equivalents.</p> <p>For example, when the VPN profile created, upon information and belief, the configuration data binary file is embedded as instructions in RAS API to be delivered to the remote computer.</p>



Source: <https://www.microsoft.com/insidetrack/blog/enabling-remote-access-with-windows-hello-for-business-in-windows-10/>

The Remote Access Service is applicable in any computing environment that uses a Wide Area Network (WAN) link or a Virtual Private Network (VPN). RAS makes it possible to connect a remote client computer to a network server over a WAN link or a VPN. The remote computer then functions on the server's LAN as though the remote computer was connected to the LAN directly. The RAS API enables programmers to access the features of RAS programmatically.

Source: <https://learn.microsoft.com/en-us/windows/win32/rras/remote-access-start-page>

The Routing and Remote Access Service (RRAS) is a Microsoft API and server software that makes it possible to create applications to administer the routing and remote access service capabilities of the operating system, to function as a network router.

Source: <https://www.netsurion.com/data-source-integrations/rras>

RAS Architecture Overview

Article • 12/06/2022 • 1 contributor

 Feedback

The Remote Access Service (RAS) enables remote workstations to establish a dial-up connection to a LAN and access resources on the LAN as if the remote workstation were on the LAN. WAN miniport drivers provide the interface between RAS and wide area network (WAN) cards such as ISDN, X.25, and Switched 56 adapters.

Source: <https://learn.microsoft.com/en-us/windows-hardware/drivers/network/ras-architecture-overview>

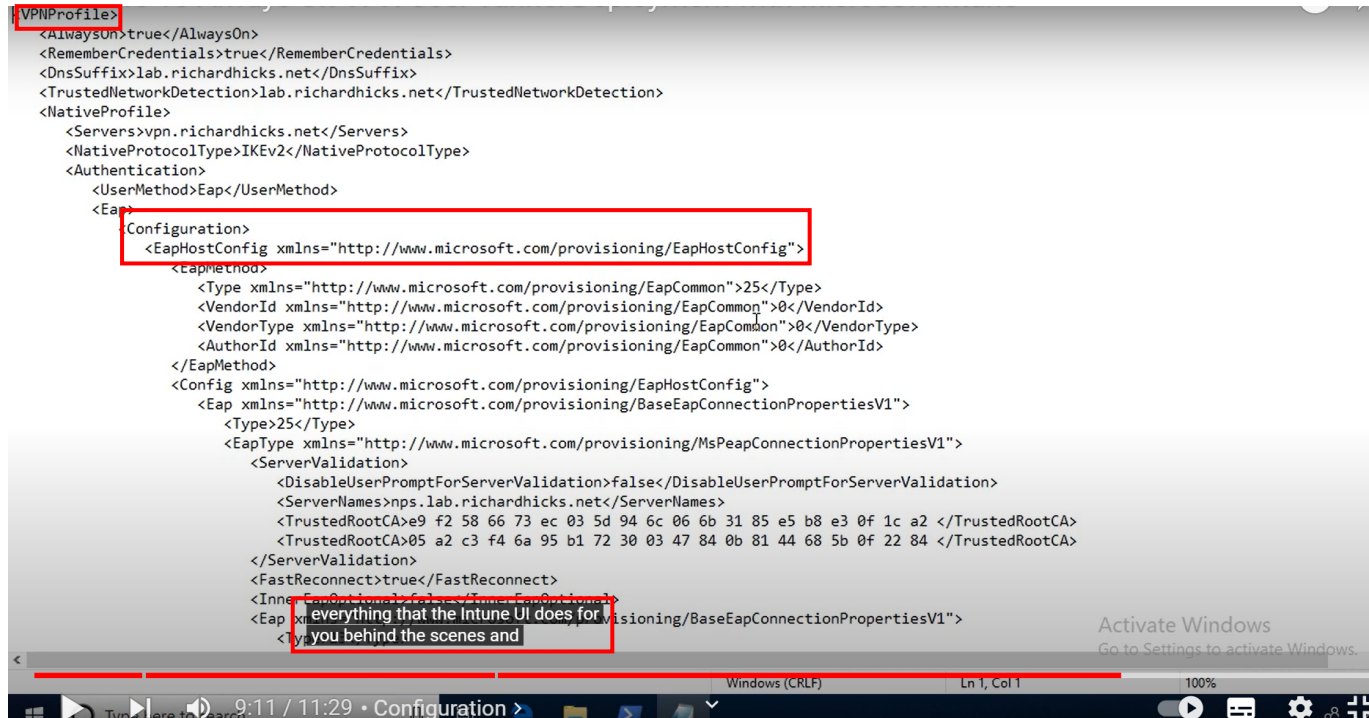
There are different VPN apps available. On user devices, you deploy the VPN app your organization uses. After the VPN app is deployed, then you create and deploy a VPN device configuration profile that configures the VPN server settings, including the VPN server name (or FQDN) and authentication method.

Source: <https://learn.microsoft.com/en-us/mem/intune/configuration/vpn-settings-configure>

Windows comes with the built-in ability to function as a VPN server, free of charge. It does this by using the point-to-point tunneling protocol (PPTP) and can be confusing to set up if you're not too tech-savvy.

Source: <https://helpdeskgeek.com/windows-10/how-to-set-up-the-windows-10-built-in-vpn-service/>

	<p>use the instructions to deploy other types of VPN. Intune supports several different protocols with the built-in Windows 10 VPN client, including IKEv2, L2TP and SSL. L2TP, SSL, and PPTP require the use of the Extensible Authentication Protocol (EAP). IKEv2 VPNs require use of EAP or machine</p> <p>Source: https://petri.com/how-to-configure-a-windows-10-vpn-profile-using-microsoft-intune/</p> <h2>Routing and Remote Access Service (RRAS)</h2> <p>Article • 08/31/2016</p> <p>The Routing and Remote Access service (RRAS) supports remote user or site-to-site connectivity by using virtual private network (VPN) or dial-up connections.</p> <p>Source: https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn614140(v=ws.11)</p> <p>Further, to the extent this element is performed at least in part by Defendant's software source code, Plaintiff shall supplement these contentions pursuant to production of such source code by the Defendant.</p>
[1.5] replacing the empty binary file of the installer program with the configuration data binary file and generating the executable file using the configuration data binary file;	<p>Defendant performs and/or induces others to perform the step of replacing the empty binary file of the installer program with the configuration data binary file and generating the executable file using the configuration data binary file.</p> <p>This element is infringed literally, or in the alternative, under the doctrine of equivalents.</p> <p>For example, when the ProfileXML file is uploaded and the admin clicks on “Create”, the empty file is replaced with configuration data to generate an executable file for the remote computer.</p>



```
<VPNProfile>
  <AlwaysOn>true</AlwaysOn>
  <RememberCredentials>true</RememberCredentials>
  <DnsSuffix>lab.richardhicks.net</DnsSuffix>
  <TrustedNetworkDetection>lab.richardhicks.net</TrustedNetworkDetection>
  <NativeProfile>
    <Servers>vpn.richardhicks.net</Servers>
    <NativeProtocolType>IKEv2</NativeProtocolType>
    <Authentication>
      <UserMethod>Eap</UserMethod>
    </Authentication>
    <Eap>
      <Configuration>
        <EapHostConfig xmlns="http://www.microsoft.com/provisioning/EapHostConfig">
          <EapMethod>
            <Type xmlns="http://www.microsoft.com/provisioning/EapCommon">25</Type>
            <VendorId xmlns="http://www.microsoft.com/provisioning/EapCommon">0</VendorId>
            <VendorType xmlns="http://www.microsoft.com/provisioning/EapCommon">0</VendorType>
            <AuthorId xmlns="http://www.microsoft.com/provisioning/EapCommon">0</AuthorId>
          </EapMethod>
          <Config xmlns="http://www.microsoft.com/provisioning/EapHostConfig">
            <Eap xmlns="http://www.microsoft.com/provisioning/BaseEapConnectionPropertiesV1">
              <Type>25</Type>
              <EapType xmlns="http://www.microsoft.com/provisioning/MsPeapConnectionPropertiesV1">
                <ServerValidation>
                  <DisableUserPromptForServerValidation>>false</DisableUserPromptForServerValidation>
                  <ServerNames>nps.lab.richardhicks.net</ServerNames>
                  <TrustedRootCA>e9 f2 58 66 73 ec 03 5d 94 6c 06 6b 31 85 e5 b8 e3 0f 1c a2 </TrustedRootCA>
                  <TrustedRootCA>05 a2 c3 f4 6a 95 b1 72 30 03 47 84 0b 81 44 68 5b 0f 22 84 </TrustedRootCA>
                </ServerValidation>
                <FastReconnect>true</FastReconnect>
              </Eap>
            </Config>
          </EapHostConfig>
        </Configuration>
      </Eap>
    </NativeProfile>
  </VPNProfile>
</Configuration>
```

everything that the Intune UI does for you behind the scenes and

Activate Windows
Go to Settings to activate Windows.

9:11 / 11:29 • Configuration > Windows (CRLF) Ln 1, Col 1 100%

Source: <https://www.youtube.com/watch?v=DQg0DLQA9ew>

Apply ProfileXML using Intune

After you configure the settings that you want using ProfileXML, you can create a custom profile in the [Microsoft Intune admin center](#). After it's created, you deploy this profile to your devices.

1. Sign in to the [Microsoft Intune admin center](#).

2. Select **Devices > Configuration profiles > Create profile**.

3. Enter the following properties:

- **Platform:** Select **Windows 10 and later**
- **Profile:** Select **Templates > Custom**.

4. Select **Create**.

5. In **Basics**, enter the following properties:

- **Name:** Enter a descriptive name for the profile. Name your profiles so you can easily identify them later.
- **Description:** Enter a description for the profile. This setting is optional, but recommended.

6. Select **Next**.

7. In **Configuration settings**, enter the following properties:

- **OMA-URI:** Enter `./user/vendor/MSFT/VPNv2/Your_VPN_profile_name_/ProfileXML`.
- **Data type:** Select `String (XML file)`.
- **Value:** Browse to, and select your XML file.

Source: <https://learn.microsoft.com/en-us/windows/security/operating-system-security/network-security/vpn/vpn-profile-options#apply-profilexml-using-intune>

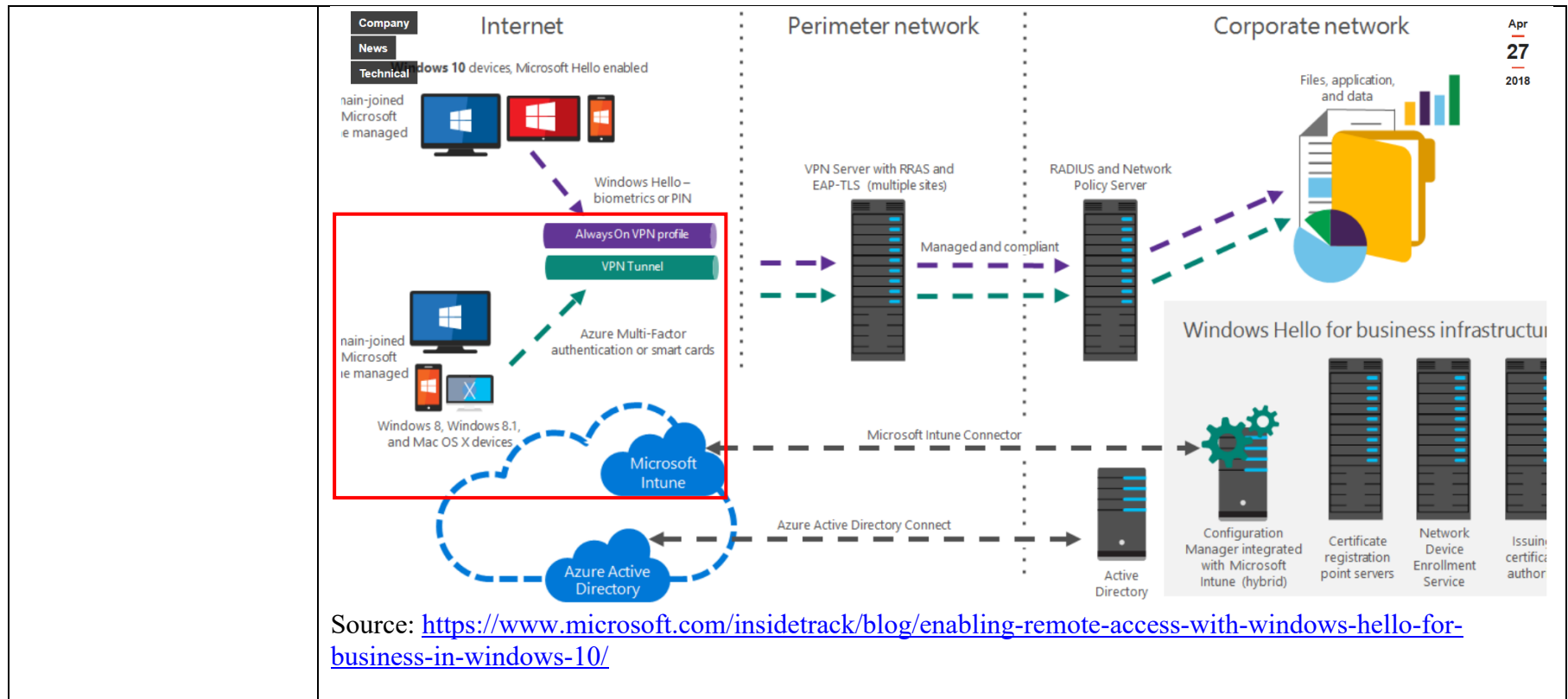
<p>[1.6] deploying the executable file comprising the configuration data binary file from the network to the remote computer;</p>	<p>Further, to the extent this element is performed at least in part by Defendant's software source code, Plaintiff shall supplement these contentions pursuant to production of such source code by the Defendant.</p> <p>Defendant performs and/or induces others to perform the step of deploying the executable file comprising the configuration data binary file from the network to the remote computer.</p> <p>This element is infringed literally, or in the alternative, under the doctrine of equivalents.</p> <p>For example, after the VPN profile is created, Intune deploys and assigns the profile to the respective remote computers including the configuration data binary file created by uploading the ProfileXML file.</p> <div data-bbox="562 600 1881 1070" data-label="Diagram"> <p>The diagram shows a cloud representing the Intune management console. Inside the cloud are three icons: an email icon labeled 'Intune email profiles', a document with a lock icon labeled 'Intune VPN profiles' (which is enclosed in a red rectangular box), and a Wi-Fi icon labeled 'Intune Wi-Fi profiles'. A large green arrow points from the cloud to a separate box on the right labeled 'Device group'. This box contains icons for a laptop and a smartphone, and it is also enclosed in a red rectangular box.</p> </div> <p>Source: https://learn.microsoft.com/en-us/mem/intune/fundamentals/deployment-plan-configuration-profile?tabs=android-disk%2Candroid-password%2Candroid-kiosk</p>
---	---

To deploy VPN settings to users in your organization, use VPN profiles in Configuration Manager. By deploying these settings, you minimize the end-user effort required to connect to resources on the company network.

For example, you want to configure all Windows 10 devices with the settings required to connect to a file share on the internal network. Create a VPN profile with the settings necessary to connect to the internal network. Then deploy this profile to all users that have devices running Windows 10. These users see the VPN connection in the list of available networks and can connect with little effort.

When you create a VPN profile, you can include a wide range of security settings. These settings include certificates for server validation and client authentication that you provision with Configuration Manager certificate profiles. For more information, see [Certificate profiles](#).

Source: <https://learn.microsoft.com/en-us/mem/configmgr/protect/deploy-use/vpn-profiles>



VPN

Many organizations deploy VPN profiles with preconfigured settings to user devices. The VPN connects your devices to your internal organization network.

If your organization uses cloud services with modern authentication and secure identities, then you probably don't need a VPN profile. Cloud-native services don't require a VPN connection.

If your apps or services aren't cloud-based or aren't cloud-native, then it's recommended to deploy a VPN profile to connect to your internal organization network.

✓ Work from anywhere

Creating a VPN profile is a common minimum baseline policy for organizations with remote workers and hybrid workers.

As users work from anywhere, they can use the VPN profile to securely connect to your organization's network to access resources.

Intune has built in VPN settings for Android, iOS/iPadOS, macOS, and Windows client devices. On user devices, your VPN connection is shown as an available connection. Users select it. And, depending on the settings in your VPN profile, users can automatically authenticate and connect to the VPN on their devices.

Source: <https://learn.microsoft.com/en-us/mem/intune/fundamentals/deployment-plan-configuration-profile?tabs=android-disk%2Candroid-password%2Candroid-kiosk>

✓ Deploy anytime

On new devices, it's recommended to deploy the VPN app during the enrollment process. When enrollment completes, then deploy the VPN device configuration policy.

If you have existing devices, deploy the VPN app at any time, and then deploy the VPN device configuration policy.

Source: <https://learn.microsoft.com/en-us/mem/intune/fundamentals/deployment-plan-configuration-profile?tabs=android-disk%2Candroid-password%2Candroid-kiosk>

For example, once the executable file is generated, it is deployed to the remote computer over the network.

Assign a policy to users or groups

1. Sign in to the Microsoft Intune admin center²⁷.
2. Select **Devices > Configuration profiles**. All the profiles are listed.
3. Select the profile you want to assign > **Properties > Assignments > Edit**:

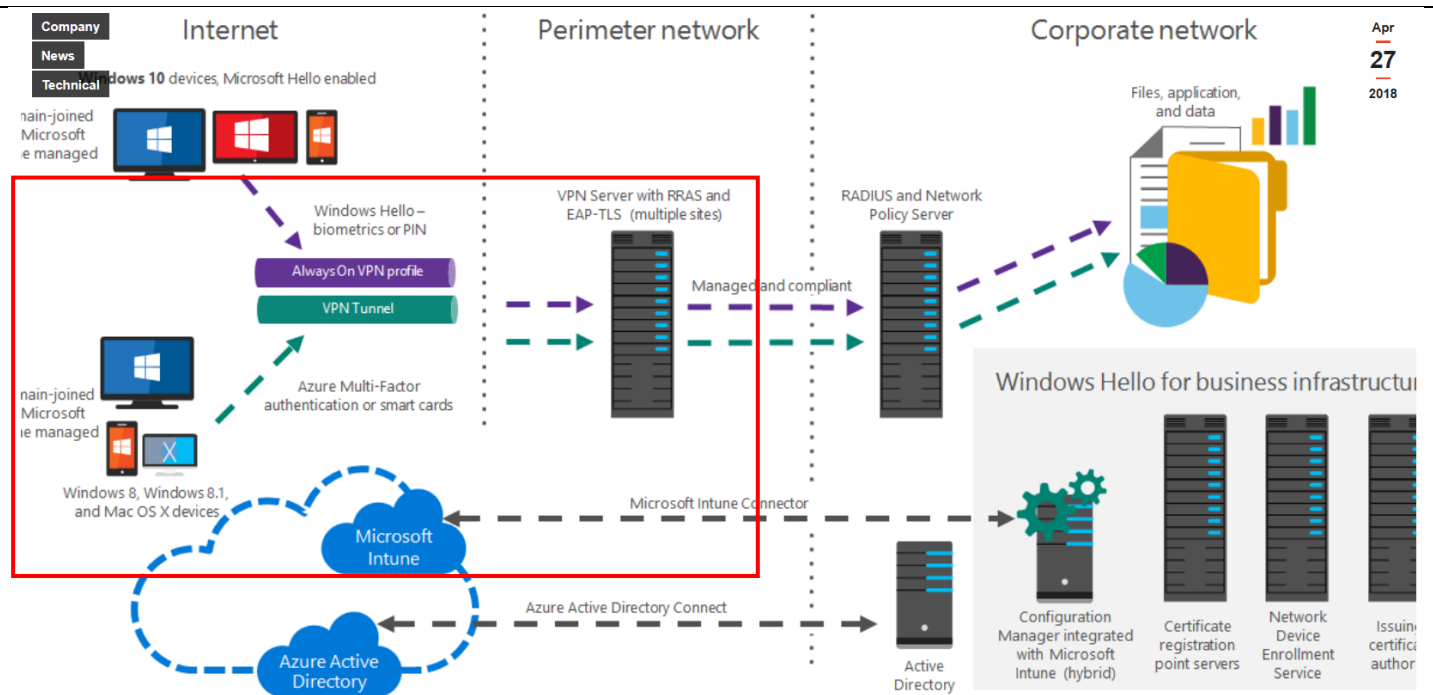
For example, to assign a device configuration profile:

- a. Go to **Devices > Configuration profiles**. All the profiles are listed.
- b. Select the policy you want to assign > **Properties > Assignments > Edit**:

Source: <https://learn.microsoft.com/en-us/mem/intune/configuration/device-profile-assign>

	<p>4. Under Included groups or Excluded groups, choose Add groups to select one or more Azure AD groups. If you intend to deploy the policy broadly to all applicable devices, select Add all users or Add all devices.</p> <div style="background-color: #f0f0f0; padding: 10px; border: 1px solid #ccc;"> <p>📘 Note</p> <p>If you select "All Devices" and "All Users", the option to add additional Azure AD groups disables.</p> </div> <p>5. Select Review + Save. This step doesn't assign your policy.</p> <p>6. Select Save. When you save, your policy is assigned. Your groups will receive your policy settings when the devices check in with the Intune service.</p> <p>Source: https://learn.microsoft.com/en-us/mem/intune/configuration/device-profile-assign</p> <p>Further, to the extent this element is performed at least in part by Defendant's software source code, Plaintiff shall supplement these contentions pursuant to production of such source code by the Defendant.</p>
<p>[1.7] executing the executable file on the remote computer to modify configuration settings of the remote computer by installing the prescribed RAS settings to edit RAS files of an operating system of the remote computer such that the remote computer is configured to establish</p>	<p>Defendant performs and/or induces others to perform the step of executing the executable file on the remote computer to modify configuration settings of the remote computer by installing the prescribed RAS settings to edit RAS files of an operating system of the remote computer such that the remote computer is configured to establish a VPN connection to access the network.</p> <p>This element is infringed literally, or in the alternative, under the doctrine of equivalents.</p> <p>For example, after the VPN profile is deployed to deliver the executable file on the remote computers, the executable file comprising configuration settings and the RAS settings configured in the RAS API are executed at the remote computer. The RAS settings modify the registry entries in the operating system, such as configurations for dial-up connection, integration with authentication servers (RADIUS), and assigning IP addresses to network interface of the remote computer.</p>

<p>a VPN connection to access the network;</p>	<p>For example, when the executable file is executed at the remote computer, the RAS client application at the remote computer uses the RasDial function that changes the phone book entries of the operating system.</p> <p>The Remote Access Service is applicable in any computing environment that uses a Wide Area Network (WAN) link or a Virtual Private Network (VPN). RAS makes it possible to connect a remote client computer to a network server over a WAN link or a VPN. The remote computer then functions on the server's LAN as though the remote computer was connected to the LAN directly. The RAS API enables programmers to access the features of RAS programmatically.</p> <p>Source: https://learn.microsoft.com/en-us/windows/win32/ras/remote-access-start-page</p> <p>Azure AD Multi-Factor Authentication platform. When combined with Remote Authentication Dial-In User Service (RADIUS) services and the Network Policy Server (NPS) extension for Azure AD Multi-Factor Authentication, VPN authentication can use strong MFA.</p> <p>Source: https://learn.microsoft.com/en-us/windows-server/remote/remote-access/overview-always-on-vpn</p>
--	--



Source: <https://www.microsoft.com/insidetrack/blog/enabling-remote-access-with-windows-hello-for-business-in-windows-10/>

RAS Architecture Overview

Article • 12/06/2022 • 1 contributor

[Feedback](#)

The Remote Access Service (RAS) enables remote workstations to establish a dial-up connection to a LAN and access resources on the LAN as if the remote workstation were on the LAN. WAN miniport drivers provide the interface between RAS and wide area network (WAN) cards such as ISDN, X.25, and Switched 56 adapters.

Source: <https://learn.microsoft.com/en-us/windows-hardware/drivers/network/ras-architecture-overview>

There are different VPN apps available. On user devices, you deploy the VPN app your organization uses. After the VPN app is deployed, then you create and deploy a VPN device configuration profile that configures the VPN server settings, including the VPN server name (or FQDN) and authentication method.

Source: <https://learn.microsoft.com/en-us/mem/intune/configuration/vpn-settings-configure>

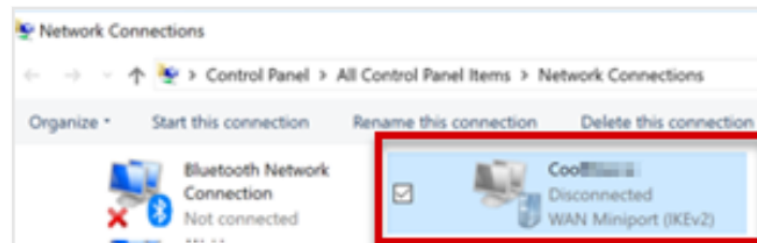
Windows comes with the built-in ability to function as a VPN server, free of charge. It does this by using the point-to-point tunneling protocol (PPTP) and can be confusing to set up if you're not too tech-savvy.

Source: <https://helpdeskgeek.com/windows-10/how-to-set-up-the-windows-10-built-in-vpn-service/>

use the instructions to deploy other types of VPN. Intune supports several different protocols with the built-in Windows 10 VPN client, including IKEv2, L2TP and SSL. L2TP, SSL, and PPTP require the use of the Extensible Authentication Protocol (EAP). IKEv2 VPNs require use of EAP or machine

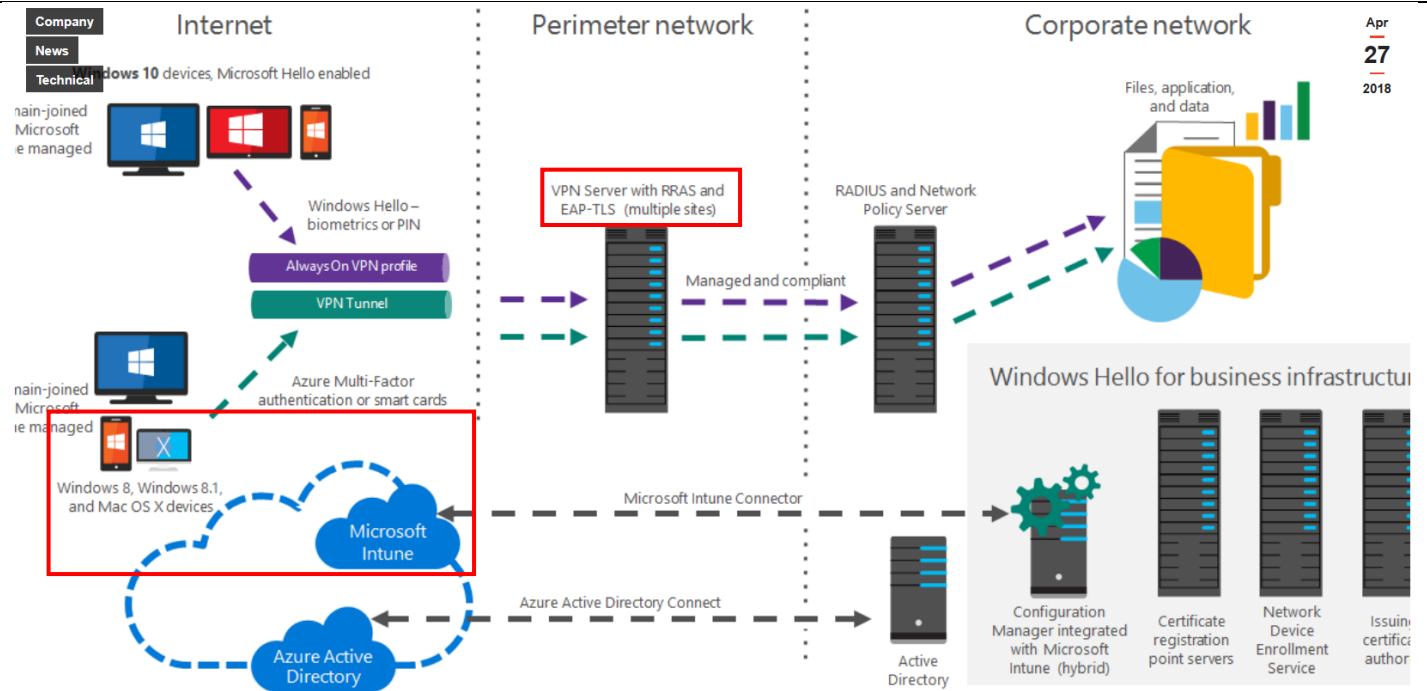
Source: <https://petri.com/how-to-configure-a-windows-10-vpn-profile-using-microsoft-intune/>

The VPN connection is listed in **Network Connections**



Source: <https://learn.microsoft.com/en-us/troubleshoot/mem/intune/device-configuration/troubleshoot-vpn-profiles?tabs=windows>

	<p>A RasDial call must specify the information that the Remote Access Connection Manager needs to establish the connection. Typically, the RasDial call provides the connection information by specifying a phone-book entry. The connection information in a phone-book entry includes phone numbers, bps rates, user authentication information, and other connection information.</p> <p>Source: https://learn.microsoft.com/en-us/windows/win32/rras/phone-book-files-and-connection-information</p> <p>Further, to the extent this element is performed at least in part by Defendant's software source code, Plaintiff shall supplement these contentions pursuant to production of such source code by the Defendant.</p>
<p>[1.8] configuring at the remote computer the RAS API as a connection application software;</p>	<p>Defendant performs and/or induces others to perform the step of configuring at the remote computer the RAS API as a connection application software</p> <p>This element is infringed literally, or in the alternative, under the doctrine of equivalents.</p> <p>For example, when the executable file is executed at the remote computer, the instructions corresponding to RAS API are executed at the remote computer to establish a VPN connection. Upon information and belief, the VPN connection is established by a connection application software configured from the RAS API instructions.</p> <p>The Remote Access Service is applicable in any computing environment that uses a Wide Area Network (WAN) link or a Virtual Private Network (VPN). RAS makes it possible to connect a remote client computer to a network server over a WAN link or a VPN. The remote computer then functions on the server's LAN as though the remote computer was connected to the LAN directly. The RAS API enables programmers to access the features of RAS programmatically.</p> <p>Source: https://learn.microsoft.com/en-us/windows/win32/rras/remote-access-start-page</p> <p>Azure AD Multi-Factor Authentication platform. When combined with Remote Authentication Dial-In User Service (RADIUS) services and the Network Policy Server (NPS) extension for Azure AD Multi-Factor Authentication, VPN authentication can use strong MFA.</p> <p>Source: https://learn.microsoft.com/en-us/windows-server/remote/remote-access/overview-always-on-vpn</p>



Source: <https://www.microsoft.com/insidetrack/blog/enabling-remote-access-with-windows-hello-for-business-in-windows-10/>

RAS Architecture Overview

Article • 12/06/2022 • 1 contributor

[Feedback](#)

The Remote Access Service (RAS) enables remote workstations to establish a dial-up connection to a LAN and access resources on the LAN as if the remote workstation were on the LAN. WAN miniport drivers provide the interface between RAS and wide area network (WAN) cards such as ISDN, X.25, and Switched 56 adapters.

Source: <https://learn.microsoft.com/en-us/windows-hardware/drivers/network/ras-architecture-overview>

	<p>There are different VPN apps available. On user devices, you deploy the VPN app your organization uses. After the VPN app is deployed, then you create and deploy a VPN device configuration profile that configures the VPN server settings, including the VPN server name (or FQDN) and authentication method.</p> <p>Source: https://learn.microsoft.com/en-us/mem/intune/configuration/vpn-settings-configure</p> <p>Windows comes with the built-in ability to function as a VPN server, free of charge. It does this by using the point-to-point tunneling protocol (PPTP) and can be confusing to set up if you're not too tech-savvy.</p> <p>Source: https://helpdeskgeek.com/windows-10/how-to-set-up-the-windows-10-built-in-vpn-service/</p> <p>use the instructions to deploy other types of VPN. Intune supports several different protocols with the built-in Windows 10 VPN client, including IKEv2, L2TP and SSL. L2TP, SSL, and PPTP require the use of the Extensible Authentication Protocol (EAP). IKEv2 VPNs require use of EAP or machine</p> <p>Source: https://petri.com/how-to-configure-a-windows-10-vpn-profile-using-microsoft-intune/</p> <p>Further, to the extent this element is performed at least in part by Defendant's software source code, Plaintiff shall supplement these contentions pursuant to production of such source code by the Defendant.</p>
[1.9] configuring at the remote computer the executable file as a self-deleting file;	<p>Defendant performs and/or induces others to perform the step of configuring at the remote computer the executable file as a self-deleting file.</p> <p>This element is infringed literally, or in the alternative, under the doctrine of equivalents.</p> <p>Upon information and belief, Intune delivers the executable file to the remote computer such that it gets deleted after the remote computer is configured for VPN.</p>

	<p>There are different VPN apps available. On user devices, you deploy the VPN app your organization uses. After the VPN app is deployed, then you create and deploy a VPN device configuration profile that configures the VPN server settings, including the VPN server name (or FQDN) and authentication method.</p> <p>Source: https://learn.microsoft.com/en-us/mem/intune/configuration/vpn-settings-configure</p> <p>Windows comes with the built-in ability to function as a VPN server, free of charge. It does this by using the point-to-point tunneling protocol (PPTP) and can be confusing to set up if you're not too tech-savvy.</p> <p>Source: https://helpdeskgeek.com/windows-10/how-to-set-up-the-windows-10-built-in-vpn-service/</p> <p>use the instructions to deploy other types of VPN. Intune supports several different protocols with the built-in Windows 10 VPN client, including IKEv2, L2TP and SSL. L2TP, SSL, and PPTP require the use of the Extensible Authentication Protocol (EAP). IKEv2 VPNs require use of EAP or machine</p> <p>Source: https://petri.com/how-to-configure-a-windows-10-vpn-profile-using-microsoft-intune/</p> <p>Further, to the extent this element is performed at least in part by Defendant's software source code, Plaintiff shall supplement these contentions pursuant to production of such source code by the Defendant.</p>
<p>[1.10.1] the step of executing the executable file further comprises: executing on the remote computer the executable file such that the RAS API functions as the connection application software that issues instructions to the remote computer to establish the</p>	<p>Defendant performs and/or induces others to perform the step of executing on the remote computer the executable file such that the RAS API functions as the connection application software that issues instructions to the remote computer to establish the VPN connection with the network.</p> <p>This element is infringed literally, or in the alternative, under the doctrine of equivalents.</p> <p>For example, when the executable file is run at the remote computer, the RAS API instructions (“connection application software”) that comprises configuration settings are run at the remote computer and a VPN connection is established between the remote computer and the network server.</p>

#: 69

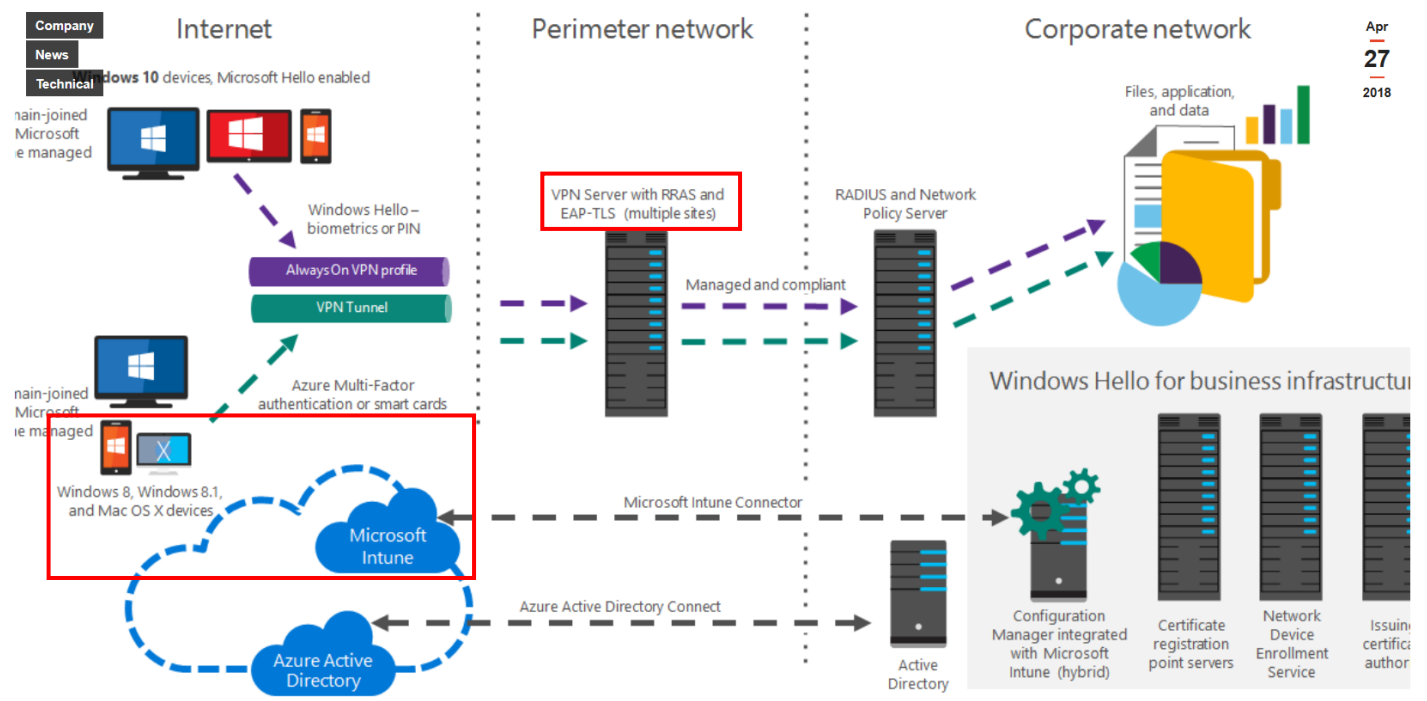
VPN connection with the network;

The Remote Access Service is applicable in any computing environment that uses a Wide Area Network (WAN) link or a Virtual Private Network (VPN). RAS makes it possible to connect a remote client computer to a network server over a WAN link or a VPN. The remote computer then functions on the server's LAN as though the remote computer was connected to the LAN directly. The RAS API enables programmers to access the features of RAS programmatically.

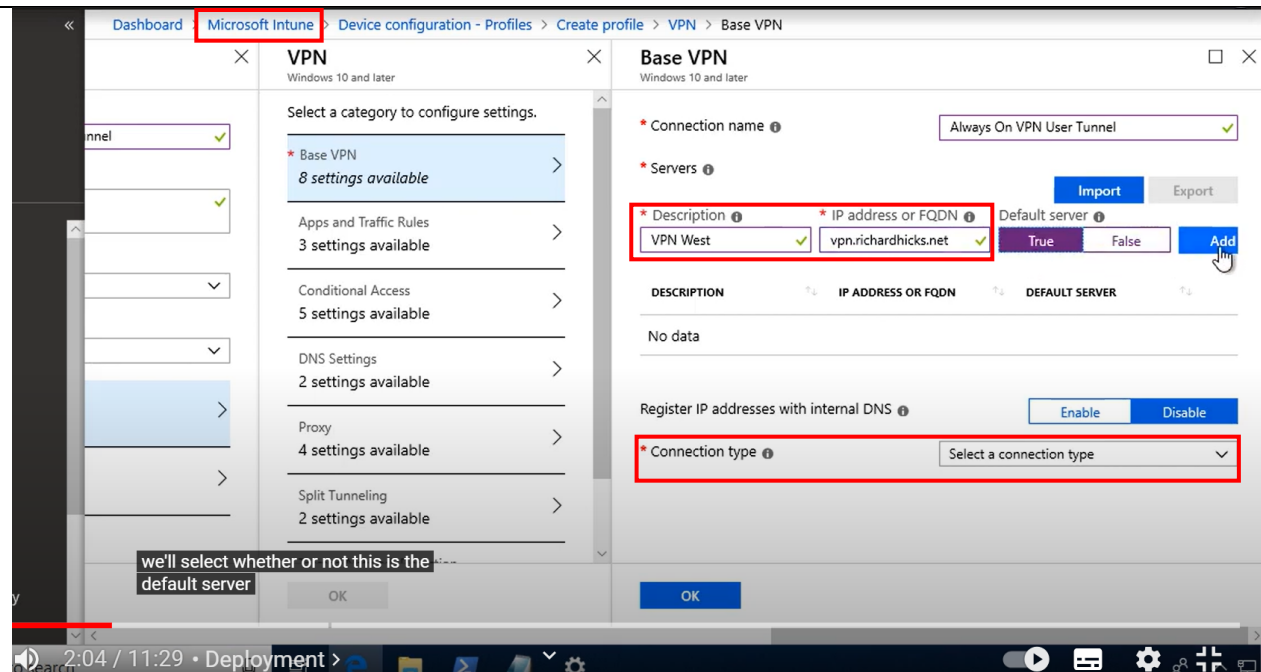
Source: <https://learn.microsoft.com/en-us/windows/win32/rras/remote-access-start-page>

Azure AD Multi-Factor Authentication platform. When combined with Remote Authentication Dial-In User Service (RADIUS) services and the Network Policy Server (NPS) extension for Azure AD Multi-Factor Authentication, VPN authentication can use strong MFA.

Source: <https://learn.microsoft.com/en-us/windows-server/remote/remote-access/overview-always-on-vpn>



	<p>Source: https://www.microsoft.com/insidetrack/blog/enabling-remote-access-with-windows-hello-for-business-in-windows-10/</p> <p>Further, to the extent this element is performed at least in part by Defendant's software source code, Plaintiff shall supplement these contentions pursuant to production of such source code by the Defendant.</p>
<p>[1.10.2] before establishing the VPN connection with a VPN server of the network, creating a connection profile that the RAS API is configured to provide to the operating system of the remote computer when the executable file is executed, wherein the connection profile contains information regarding at least one of an IP address, an address for a gateway, a DNS address, a WINS address, a DHCP address, and a NAT address;</p>	<p>Defendant performs and/or induces others to perform the step of before establishing the VPN connection with a VPN server of the network, creating a connection profile that the RAS API is configured to provide to the operating system of the remote computer when the executable file is executed, wherein the connection profile contains information regarding at least one of an IP address, an address for a gateway, a DNS address, a WINS address, a DHCP address, and a NAT address.</p> <p>This element is infringed literally, or in the alternative, under the doctrine of equivalents.</p> <p>For example, when Intune deploys the VPN profile comprising configuration settings at the remote computer, the executable file created using RAS API instructions is executed at the remote computer. Upon information and belief, before establishing a connection with the VPN server, the RAS API instructions generate a connection profile including settings related to connection type (multiple types of connections building the “connection profile”) and the profile is provided to the Windows operating system in the remote computer. Further, Intune created the VPN profile using PublicXML file which comprises DNS Servers Address. Therefore, the connection profile provided to the Windows operating system comprises at least the DNS server address.</p>



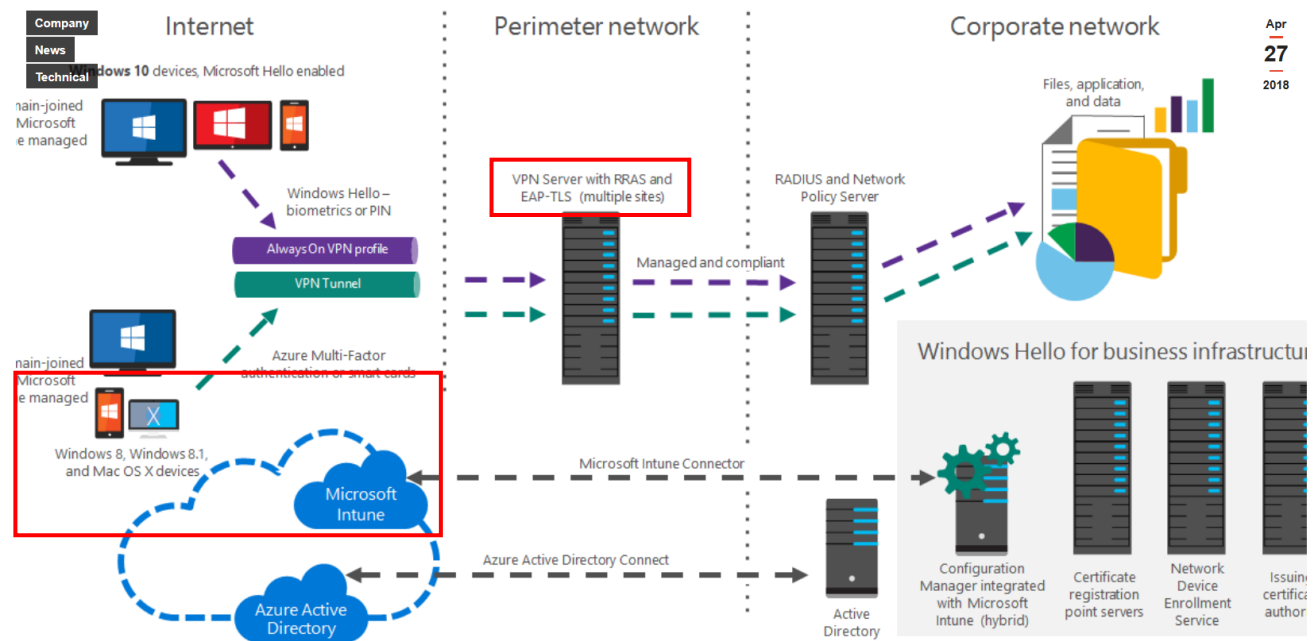
Source: <https://www.youtube.com/watch?v=DQg0DLQA9ew> ; at 2:04

The Remote Access Service is applicable in any computing environment that uses a Wide Area Network (WAN) link or a Virtual Private Network (VPN). RAS makes it possible to connect a remote client computer to a network server over a WAN link or a VPN. The remote computer then functions on the server's LAN as though the remote computer was connected to the LAN directly. The RAS API enables programmers to access the features of RAS programmatically.

Source: <https://learn.microsoft.com/en-us/windows/win32/rras/remote-access-start-page>

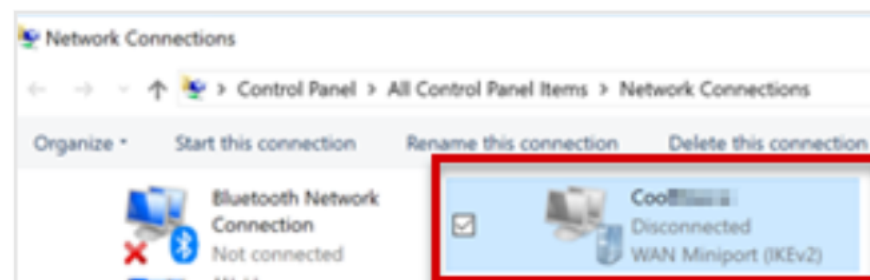
Azure AD Multi-Factor Authentication platform. When combined with Remote Authentication Dial-In User Service (RADIUS) services and the Network Policy Server (NPS) extension for Azure AD Multi-Factor Authentication, VPN authentication can use strong MFA.

Source: <https://learn.microsoft.com/en-us/windows-server/remote/remote-access/overview-always-on-vpn>



Source: <https://www.microsoft.com/insidetrack/blog/enabling-remote-access-with-windows-hello-for-business-in-windows-10/>

The VPN connection is listed in **Network Connections**



Source: <https://learn.microsoft.com/en-us/troubleshoot/mem/intune/device-configuration/troubleshoot-vpn-profiles?tabs=windows>

- **Register IP addresses with internal DNS:** Select **Enable** to configure the VPN profile to dynamically register the IP addresses assigned to the VPN interface with the internal DNS. Select **Disable** to not dynamically register the IP addresses.

Source: <https://learn.microsoft.com/en-us/mem/intune/configuration/vpn-settings-windows-10>

Connection type

- **Connection type:** Select the VPN connection type from the following list of vendors:
 - Check Point Capsule VPN
 - Cisco AnyConnect
 - Citrix
 - F5 Access
 - Palo Alto Networks GlobalProtect
 - Pulse Secure
 - SonicWall Mobile Connect
 - Automatic (Native type)
 - IKEv2 (Native type)
 - L2TP (Native type)
 - PPTP (Native type)

Source: <https://learn.microsoft.com/en-us/mem/intune/configuration/vpn-settings-windows-10>

	<div data-bbox="562 248 1774 873" data-label="Code-Block"> <pre>PowerShell # Define key VPN profile parameters # Replace with your own values \$Domain = 'corp' # Name of the domain. \$TemplateName = 'Contoso VPN' # Name of the test VPN connection you created in the tutorial. \$ProfileName = 'Contoso AlwaysOn VPN' # Name of the profile we are going to create. \$Servers = 'aov-vpn.contoso.com' #Public or routable IP address or DNS name for the VPN gateway. \$DnsSuffix = 'corp.contoso.com' # Specifies one or more commas separated DNS suffixes. \$DomainName = '.corp.contoso.com' #Used to indicate the namespace to which the policy applies. Contains \$DNSServers = '10.10.0.6' #List of comma-separated DNS Server IP addresses to use for the namespace. \$TrustedNetwork = 'corp.contoso.com' #Comma-separated string to identify the trusted network.</pre> </div> <p>Source: https://learn.microsoft.com/en-us/windows-server/remote/remote-access/tutorial-aovpn-deploy-configure-client</p> <p>Further, to the extent this element is performed at least in part by Defendant's software source code, Plaintiff shall supplement these contentions pursuant to production of such source code by the Defendant.</p>
<p>[1.10.3] coding WAN login credentials and automatically transmitting the WAN login credentials from the remote computer to the VPN server of the network when executing the executable file;</p>	<p>Defendant performs and/or induces others to perform the step of coding WAN login credentials and automatically transmitting the WAN login credentials from the remote computer to the VPN server of the network when executing the executable file.</p> <p>This element is infringed literally, or in the alternative, under the doctrine of equivalents.</p> <p>For example, Always ON VPN functionality (added to the VPN profile in Intune admin center) establishes VPN connection by creating VPN user tunnel for Virtual WAN. Upon information and belief, WAN login credentials are coded in the executable file and transmitted to the remote computer for creating the VPN user tunnel.</p>

Configure an Always On VPN user tunnel for Virtual WAN

Article • 05/27/2021 • 1 contributor

 Feedback

In this article

[Prerequisites](#)

[Configure a user tunnel](#)

[To remove a profile](#)

[Next steps](#)

A new feature of the Windows 10 or later VPN client, Always On, is the ability to maintain a VPN connection. With Always On, the active VPN profile can connect automatically and remain connected based on triggers, such as user sign-in, network state change, or device screen active.

You can use gateways with Always On to establish persistent user tunnels and device tunnels to Azure.

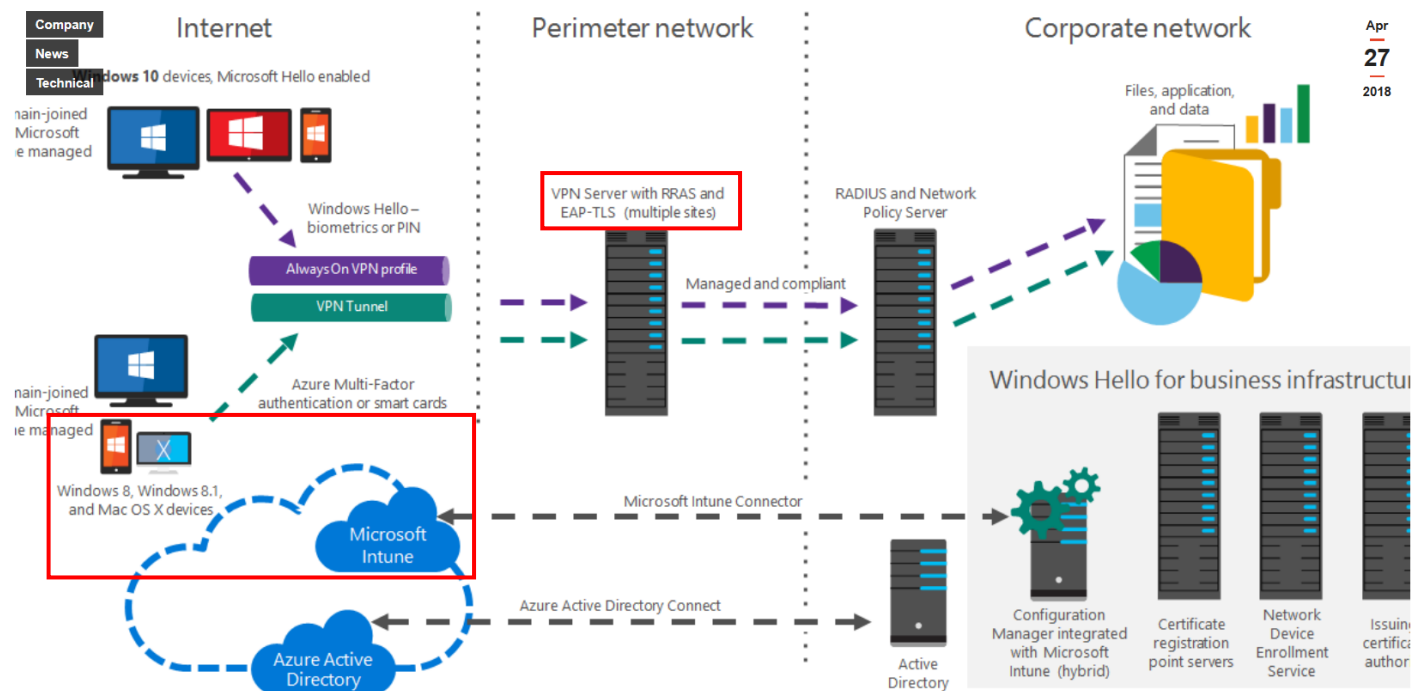
Always On VPN connections include either of two types of tunnels:

- **Device tunnel:** Connects to specified VPN servers before users sign in to the device. Pre-sign-in connectivity scenarios and device management use a device tunnel.
- **User tunnel:** Connects only after users sign in to the device. By using user tunnels, you can access organization resources through VPN servers.

Source: <https://learn.microsoft.com/en-us/azure/virtual-wan/howto-always-on-user-tunnel>

- **Routing.** RRAS is a software router and an open platform for routing and networking. It offers routing services to businesses in local area network (LAN) and wide area network (WAN) environments or over the Internet by using secure VPN connections. Routing is used for multiprotocol LAN-to-LAN, LAN-to-WAN, VPN, and network address translation (NAT) routing services.

Source: [https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn614140\(v=ws.11\)](https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn614140(v=ws.11))



Source: <https://www.microsoft.com/insidetrack/blog/enabling-remote-access-with-windows-hello-for-business-in-windows-10/>

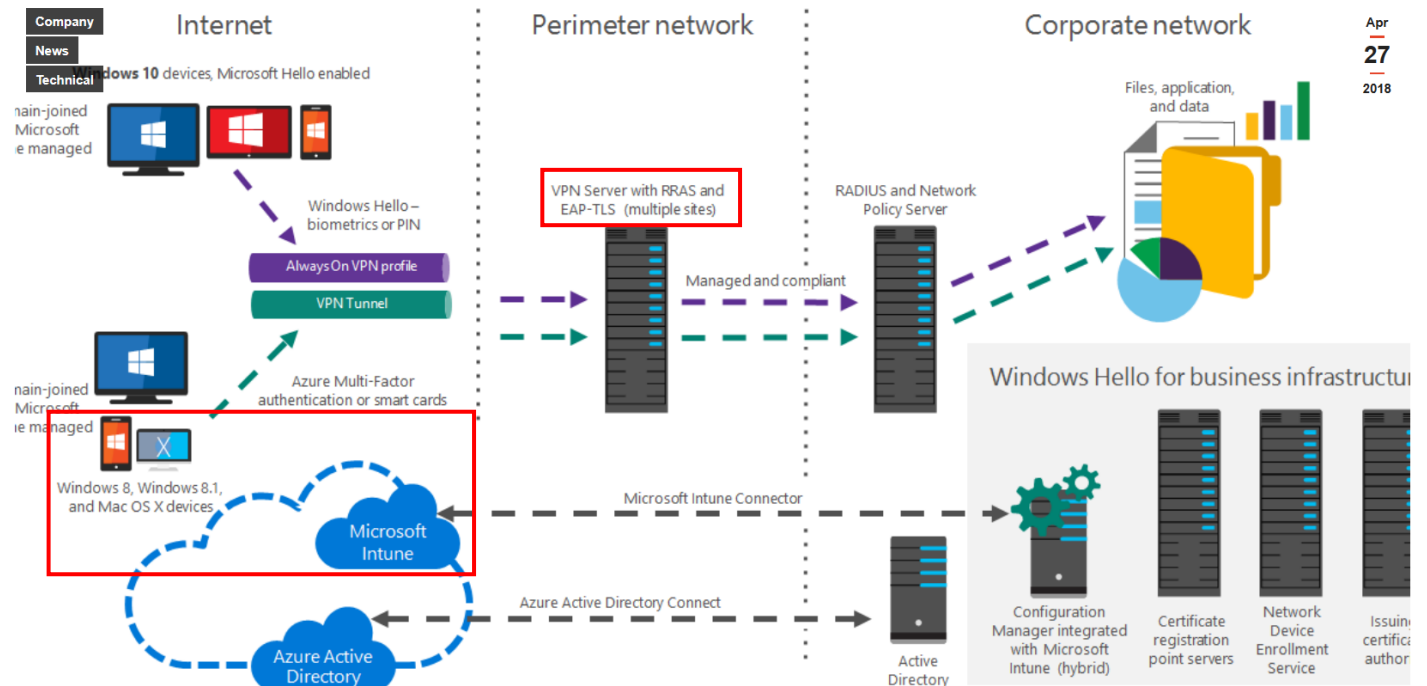
	Further, to the extent this element is performed at least in part by Defendant's software source code, Plaintiff shall supplement these contentions pursuant to production of such source code by the Defendant.
[1.10.4] coding LAN login credentials and automatically transmitting the LAN login credentials from the remote computer to a domain controller of the network when executing the executable file;	<p>Defendant performs and/or induces others to perform the step of coding LAN login credentials and automatically transmitting the LAN login credentials from the remote computer to a domain controller of the network when executing the executable file.</p> <p>This element is infringed literally, or in the alternative, under the doctrine of equivalents.</p> <p>For example, the VPN profile deployed at the remote computer configures the remote computer to establish connection to the VPN server with RRAS server. The connection to RRAS server includes LAN-to-LAN connections such that the remote computer connects to a LAN network. Upon information and belief, LAN login credentials are coded in the executable file and transmitted to the remote computer for connecting to the LAN network.</p> <p>RRAS</p> <p>We use Routing and Remote Access Service (RRAS) to deploy VPN, dial-up remote access services, multiprotocol LAN-to-LAN, LAN-to-WAN, and network address translation (NAT) routing services.</p> <p>For more information about deploying VPN using RRAS, see Routing and Remote Access Service (RRAS).</p> <p>Source: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWrCne</p> <ul style="list-style-type: none"> • Routing. RRAS is a software router and an open platform for routing and networking. It offers routing services to businesses in local area network (LAN) and wide area network (WAN) environments or over the Internet by using secure VPN connections. Routing is used for multiprotocol LAN-to-LAN, LAN-to-WAN, VPN, and network address translation (NAT) routing services. <p>Source: https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn614140(v=ws.11)</p>

	<div data-bbox="567 243 1963 925"> </div> <p>Source: https://www.microsoft.com/insidetrack/blog/enabling-remote-access-with-windows-hello-for-business-in-windows-10/</p> <p>Further, to the extent this element is performed at least in part by Defendant's software source code, Plaintiff shall supplement these contentions pursuant to production of such source code by the Defendant.</p>
<p>[1.10.5] wherein the WAN and the LAN login credentials are coded in a manner that the WAN and LAN login credentials are unknown to the user in order to prevent the user from becoming aware of</p>	<p>Defendant performs and/or induces others to perform the step of coding of coding WAN and the LAN login credentials in a manner that the WAN and LAN login credentials are unknown to the user in order to prevent the user from becoming aware of the code of the WAN and LAN login credentials.</p> <p>This element is infringed literally, or in the alternative, under the doctrine of equivalents.</p> <p>For example, when the remote computer is configured to connect with VPN server, upon information and belief, the LAN and WAN credentials are automatically transmitted to establish the connection without displaying them to the user of the remote computer.</p>

the code of the WAN and LAN login credentials;

- **Routing.** RRAS is a software router and an open platform for routing and networking. It offers routing services to businesses in local area network (LAN) and wide area network (WAN) environments or over the Internet by using secure VPN connections. Routing is used for multiprotocol LAN-to-LAN, LAN-to-WAN, VPN, and network address translation (NAT) routing services.

Source: [https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn614140\(v=ws.11\)](https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn614140(v=ws.11))



Source: <https://www.microsoft.com/insidetrack/blog/enabling-remote-access-with-windows-hello-for-business-in-windows-10/>

	<div><h2>RAS Architecture Overview</h2><div>Article • 12/06/2022 • 1 contributor</div><div>Feedback</div><p>The Remote Access Service (RAS) enables remote workstations to establish a dial-up connection to a LAN and access resources on the LAN as if the remote workstation were on the LAN. WAN miniport drivers provide the interface between RAS and wide area network (WAN) cards such as ISDN, X.25, and Switched 56 adapters.</p><p>Source: https://learn.microsoft.com/en-us/windows-hardware/drivers/network/ras-architecture-overview</p><p>Further, to the extent this element is performed at least in part by Defendant's software source code, Plaintiff shall supplement these contentions pursuant to production of such source code by the Defendant.</p></div>
<div>[1.11] automatically deleting the executable file from the remote computer after terminating the VPN connection.</div>	<div><p>Defendant performs and/or induces others to perform the step of configuring at the remote computer the executable file as a self-deleting file.</p><p>This element is infringed literally, or in the alternative, under the doctrine of equivalents.</p><p>For example, upon information and belief, the Windows operating system running on the remote computers executes “Remove-VpnConnection” command to terminate the VPN connection and remove the executable files received from the Intune admin center.</p></div>

Remove-VpnConnection

Reference

Feedback

Module: [VpnClient](#)

Removes specified VPN connection profiles.

Syntax

PowerShellCopy

```
Remove-VpnConnection
    [-Name] <String[]>
    [-Force]
    [-PassThru]
    [-AllUserConnection]
    [-CimSession <CimSession[]>]
    [-ThrottleLimit <Int32>]
    [-AsJob]
    [-WhatIf]
    [-Confirm]
    [<CommonParameters>]
```

Source: <https://learn.microsoft.com/en-us/powershell/module/vpnclient/remove-vpnconnection?view=windowsserver2019-ps>

Further, to the extent this element is performed at least in part by Defendant's software source code, Plaintiff shall supplement these contentions pursuant to production of such source code by the Defendant.

2. List of References

1. <https://learn.microsoft.com/en-us/mem/intune/fundamentals/what-is-intune>, last accessed on July 7, 2023.
2. <https://learn.microsoft.com/en-us/mem/endpoint-manager-overview>, last accessed on July 7, 2023.
3. <https://learn.microsoft.com/en-us/mem/intune/configuration/vpn-settings-windows-10>, last accessed on July 7, 2023.
4. <https://www.youtube.com/watch?v=nEa5AFBCRbI>, last accessed on July 7, 2023.
5. <https://learn.microsoft.com/en-us/managed-desktop/prepare/access-admin-center>, last accessed on July 7, 2023.
6. <https://learn.microsoft.com/en-us/mem/intune/configuration/vpn-settings-configure>, last accessed on July 7, 2023.
7. <https://learn.microsoft.com/en-us/windows/security/operating-system-security/network-security/vpn/vpn-profile-options#apply-profilexml-using-intune>, last accessed on July 7, 2023.
8. <https://learn.microsoft.com/en-us/windows-server/remote/remote-access/tutorial-aovpn-deploy-configure-client>, last accessed on July 7, 2023.
9. <https://www.netsurion.com/data-source-integrations/rras>, last accessed on July 7, 2023.
10. [https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn614140\(v=ws.11\)](https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn614140(v=ws.11)), last accessed on July 7, 2023.
11. <https://learn.microsoft.com/en-us/mem/intune/configuration/device-profile-assign>, last accessed on July 7, 2023.
12. <https://learn.microsoft.com/en-us/windows/win32/rras/phone-book-files-and-connection-information>, last accessed on July 7, 2023.
13. <https://learn.microsoft.com/en-us/windows-hardware/drivers/ifs/delete-on-close>, last accessed on July 7, 2023.
14. <https://learn.microsoft.com/en-us/windows/win32/rras/ras-phone-books>, last accessed on July 7, 2023.
15. <https://directaccess.richardhicks.com/tag/rasphone/>, last accessed on July 7, 2023.
16. <https://learn.microsoft.com/en-us/windows-hardware/drivers/network/ras-architecture-overview>, last accessed on July 7, 2023.
17. <https://helpdeskgeek.com/windows-10/how-to-set-up-the-windows-10-built-in-vpn-service/>, last accessed on July 7, 2023.
18. <https://petri.com/how-to-configure-a-windows-10-vpn-profile-using-microsoft-intune/>, last accessed on July 7, 2023.
19. <https://www.youtube.com/watch?v=DQg0DLQA9ew>, last accessed on July 7, 2023.
20. <https://learn.microsoft.com/en-us/windows/win32/rras/remote-access-start-page>, last accessed on July 7, 2023.
21. <https://learn.microsoft.com/en-us/windows-server/remote/remote-access/overview-always-on-vpn>, last accessed on July 7, 2023.
22. <https://www.microsoft.com/insidetrack/blog/enabling-remote-access-with-windows-hello-for-business-in-windows-10/>, last accessed on July 7, 2023.
23. <https://learn.microsoft.com/en-us/mem/configmgr/protect/deploy-use/vpn-profiles>, last accessed on July 7, 2023.
24. <https://learn.microsoft.com/en-us/mem/intune/fundamentals/deployment-plan-configuration-profile?tabs=android-disk%2Candroid-password%2Candroid-kiosk>, last accessed on July 7, 2023.

25. <https://learn.microsoft.com/en-us/troubleshoot/mem/intune/device-configuration/troubleshoot-vpn-profiles?tabs=windows>, last accessed on July 7, 2023.
26. <https://directaccess.richardhicks.com/tag/rasphone/>, last accessed on July 7, 2023.
27. <https://learn.microsoft.com/en-us/windows/win32/rras/ras-phone-books>, last accessed on July 7, 2023.
28. <https://learn.microsoft.com/en-us/mem/intune/configuration/vpn-settings-configure#step-2---create-the-profile>, last accessed on July 7, 2023.
29. <https://www.securew2.com/blog/what-is-eap-tls>, last accessed on July 7, 2023.